Równania diofantyczne i arytmetyka modularna

dr inż. Bartłomiej Pawlik

1 maja 2024

Liniowe równania diofantyczne

Definicja

Równaniem diofantycznym nazywamy dowolne równanie typu

$$f(x_1, x_2, \ldots, x_n) = 0,$$

w którym szukane rozwiązanie składa się z liczb całkowitych.

Definicja

Niech $a_1, a_2, \ldots, a_n \in \mathbb{Z}/\{0\}$ i niech $b \in \mathbb{Z}$. Równanie diofantyczne postaci

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = b$$

o niewiadomych $x_1, x_2, \ldots, x_n$ nazywamy **liniowym równaniem diofantycznym**, a liczby $a_1, a_2, \ldots, a_n$ nazywamy współczynnikami.

Twierdzenie

1. Równanie diofantyczne $ax + by = c$ o niewiadomych x i y ma rozwiązanie, wtedy i tylko wtedy, gdy $\mathrm{NWD}(a, b) | c$.
2. Jeżeli para x_0, y_0 jest rozwiązaniem równania diofantycznego $ax + by = c$, to wszystkie rozwiązania tego równania dane są wzorami

$$x = x_0 + \frac{b}{\mathrm{NWD}(a, b)} \cdot t, \qquad y = y_0 - \frac{a}{\mathrm{NWD}(a, b)} \cdot t,$$

gdzie $t \in \mathbb{Z}$.

Arytmetyka modularna

Definicja

Niech $m \in \mathbb{N}/\{1\}$ i $a, b \in \mathbb{Z}$.

- a **przystaje do** b **modulo** m, gdy a i b mają taką samą resztę z dzielenia przez m, co zapisujemy $a \equiv_m b$ lub $a = b \mod m$.
- W przeciwnym przypadku mówimy, że a **nie przystaje do** b **modulo** m, co zapisujemy $a \not\equiv_m b$ lub $a \neq b \mod m$.
- Liczbę m nazywamy **modułem**.

Przykład

$15 \equiv_{12} 3, \ 15 \not\equiv_{12} 7$
$15 \equiv_4 3, \ 15 \equiv_4 7$

Stwierdzenie

$a \equiv_m b$ wtedy i tylko wtedy, gdy $m | (a - b)$.

Stwierdzenie

Relacja przystawania modulo m w pierścieniu liczb całkowitych jest **kongruencją**, to znaczy jest relacją równoważności (zwrotna, symetryczna, przechodnia) oraz dla dowolnych liczb całkowitych a, b, c, d takich, że $a \equiv_m b$ i $c \equiv_m d$ zachodzi

- $(a + c) \equiv_m (b + d)$
- $ac \equiv_m bd$

Z definicji przystawania modulo m oraz z twierdzenia o dzieleniu z resztą wynika, że każda liczba całkowita przystaje modulo m dokładnie do jednej liczby ze zbioru reszt z dzielenia przez m, czyli zbioru $\{0, 1, \ldots, m - 1\}$. Każda z tych reszt określa klasę abstrakcji relacji przystawania.

Przykład

Klasy abstrakcji przystawania modulo 3:

$$[0]_3 = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$$
$$[1]_3 = \{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\}$$
$$[2]_3 = \{\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots\}$$

Na zbiorze $\mathbb{Z}_m$ klas abstrakcji relacji przystawania modulo m definiujemy działania

- dodawanie modulo m:

$$[a]_m +_m [b]_m = [a+b]_m$$

- mnożenie modulo m:

$$[a]_m \cdot_m [b]_m = [a \cdot b]_m$$

Przykład

$5 +_6 2 = 1, \; 4 \cdot_8 6 = 0.$

Twierdzenie

Zbiór $\mathbb{Z}_m$ klas abstrakcji relacji przystawania modulo m z działaniami dodawania modulo m i mnożenia modulo m jest pierścieniem przemiennym z jedynką, który nazywamy **pierścieniem reszt modulo** m.

Przykład

W pierścieniu $\mathbb{Z}_6$ obliczyć $2+4$, $1-3$, -3, 5^{-1} oraz 2^{-1}.

$$\begin{aligned} 2+4 &= 0 \quad (\text{ponieważ } 6 \equiv_6 0) \\ 1-3 &= 4 \quad (\text{ponieważ } -2 \equiv_6 4) \\ -3 &= 3 \quad (\text{ponieważ } -3 \equiv_6 3) \\ 5^{-1} &= 5 \quad (\text{ponieważ } 5 \cdot 5 = 25 \equiv_6 1) \end{aligned}$$

2^{-1} nie istnieje, gdyż każdy z iloczynów $2 \cdot 0$, $2 \cdot 1$, $2 \cdot 2$, $2 \cdot 3$, $2 \cdot 4$ i $2 \cdot 5$ nie przystaje do 1 modulo 6.

Stwierdzenie

Element $a \in \mathbb{Z}_m$ jest odwracalny wtedy i tylko wtedy, gdy $a \perp m$.
W szczególności, pierścień reszt modulo m jest ciałem wtedy i tylko wtedy, gdy m jest liczbą pierwszą.

Definicja

Równanie w pierścieniu reszt modulo m nazywamy **równaniem modularnym**.

Zauważmy, że <u>każde</u> równanie modularne można traktować jako równanie diofantyczne. Wynika to z faktu, że $a \equiv_m b$ wtedy i tylko wtedy, gdy istnieje liczba całkowita k taka, że $a + mk = b$.

Twierdzenie

- Równanie $ax = b$ ma rozwiązanie w $\mathbb{Z}_m$ wtedy i tylko wtedy, gdy $\mathrm{NWD}(a, m) | b$.
- Jeżeli x_0 jest rozwiązaniem równania $ax = b$ w $\mathbb{Z}_m$, to liczba różnych rozwiązań tego równania w $\mathbb{Z}_m$ wynosi $\mathrm{NWD}(a, m)$ oraz każde rozwiązanie ma postać

$$x_t = x_0 +_m t \cdot \frac{m}{\mathrm{NWD}(a, m)}$$

dla $t \in \{0, 1, \ldots, \mathrm{NWD}(a, m) - 1\}$.

Twierdzenie

Niech $a, b, c, d \in \mathbb{Z}$ i $m, k \in \mathbb{N}/\{1\}$.

- $a \equiv_m b$ wtedy i tylko wtedy, gdy $ak \equiv_{mk} bk$.
- Jeżeli $a \equiv_m b$, to $ac \equiv_m bc$.
- Jeżeli $ac \equiv_m bc$ oraz $c \perp m$, to $a \equiv_m b$.
- Jeżeli $a \equiv_{mk} b$, to $a \equiv_m b$ oraz $a \equiv_k b$.
- Jeżeli $a \equiv_m b$ oraz $a \equiv_k b$ oraz $m \perp k$, to $a \equiv_{mk} b$.

Przykład

Obliczyć 7^{-1} w $\mathbb{Z}_{15}$.
Szukamy rozwiązania równania $7x = 1$ w $\mathbb{Z}_{15}$. Zauważmy, że rozwiązanie istnieje, ponieważ $7 \perp 15$.
Mnożąc obustronnie równanie $7x \equiv_{15} 1$ przez 2 otrzymujemy

$$14x \equiv_{15} 2,$$

a z faktu $14 \equiv_{15} -1$ otrzymujemy

$$-1 \cdot x \equiv_{15} 2,$$

więc

$$x \equiv_{15} -2 \equiv_{15} 13.$$

Ostatecznie $7^{-1} = 13$ w $\mathbb{Z}_{15}$.
Sprawdzenie wyniku: $7 \cdot 13 = 91 = 6 \cdot 15 + 1$.

Przykład

Rozwiązać równanie $10x + 9 = 17$ w $\mathbb{Z}_{24}$.
Po obustronnym odjęciu liczby 9 otrzymujemy $10x \equiv_{24} 8$.
Zauważmy, że $\mathrm{NWD}(10, 24) = 2$, więc - po pierwsze - równanie jest rozwiązywalne (gdyż $2|8$) oraz - po drugie - posiada dokładnie 2 rozwiązania w $\mathbb{Z}_{24}$.
Mnożąc otrzymane równanie obustronnie przez 5 dostajemy

$$50x \equiv_{24} 40,$$

więc (biorąc pod uwagę, że $50 \equiv_{24} 2$ i $40 \equiv_{24} 16$) mamy

$$2x \equiv_{24} 16.$$

Nietrudno zauważyć, że jednym z rozwiązań ostatniego równania jest $x_0 = 8$.
Drugie równanie ma postać

$$x_1 = x_0 +_{24} 1 \cdot \frac{24}{\mathrm{NWD}(10, 24)} = 8 +_{24} 1 \cdot \frac{24}{2} = 20,$$

więc ostatecznie rozwiązaniami zadania są liczby 8 oraz 20.

Twierdzenie Eulera

Dla $a \in \mathbb{Z}$ i $m \in \mathbb{N}/\{1\}$ takich, że $a \perp m$ zachodzi

$$a^{\varphi(m)} \equiv_m 1.$$

Małe twierdzenie Fermata

Dla $a \in \mathbb{Z}$ i $p \in \mathbb{P}$ takich, że $a \perp p$ zachodzi

$$a^{p-1} \equiv_p 1.$$

Przykład

Wyznaczyć ostatnią cyfrę liczby 7^{2022}.
Zadanie jest równoważne z określeniem wartości liczby 7^{2022} modulo 10.
Zauważmy, że

$$7^2 = 49 \equiv_{10} 9 \equiv_{10} (-1).$$

Zatem

$$7^{2022} \equiv_{10} (7^2)^{1011} \equiv_{10} (-1)^{1011} = -1 \equiv_{10} 9.$$

Ostatnią cyfrą liczby 7^{2022} jest 9.

Algorytm szybkiego potęgowania modularnego

Algorytm służy do obliczania wartości a^n w $\mathbb{Z}_m$ dla dużych wartości m i n. Polega on na iteracyjnym obliczaniu wartości (modulo m) funkcji rekurencyjnej

$$G(n) = \begin{cases} a & \text{dla } n = 1 \\ \left(G\left(\frac{n}{2}\right)\right)^2 & \text{dla } n = 2k \\ a \cdot \left(G\left(\frac{n-1}{2}\right)\right)^2 & \text{dla } n = 2k+1 \end{cases}$$

gdzie k jest liczbą całkowitą dodatnią.

- $w := a$
- Obliczyć reprezentację binarną liczby n, czyli $n = (1n_s n_{s-1} \cdots n_1 n_0)_2$
- Dla wszystkich $k \in \{s, s-1, \ldots, 1, 0\}$ wykonać w $\mathbb{Z}_m$
  - jeżeli $n_k = 0$, to $w \leftarrow w^2$
  - jeżeli $n_k = 1$, to $w \leftarrow a \cdot w^2$
- $a^n = w$

Przykład (pierwszy sposób)

Wyznaczyć przedostatnią cyfrę liczby 7^{2022}.
Aby rozwiązać zadanie wystarczy obliczyć wartość wyrażenia 7^{2022} modulo 100.
Wykładnik reprezentujemy w postaci binarnej: $2022 = 11111100110_2$.
Wypisujemy w tabeli cyfry reprezentacji binarnej od końca i wykonujemy działania:

1	$w = 7$
1	$w = 7 \cdot 7^2 = 343 \equiv_{100} 43$
1	$w = 7 \cdot 43^2 = 12943 \equiv_{100} 43$
1	$w = 7 \cdot 43^2 = 12943 \equiv_{100} 43$
1	$w = 7 \cdot 43^2 = 12943 \equiv_{100} 43$
1	$w = 7 \cdot 43^2 = 12943 \equiv_{100} 43$
0	$w = 43^2 = 1849 \equiv_{100} 49$
0	$w = 49^2 = 2401 \equiv_{100} 1$
1	$w = 7 \cdot 1^2 = 7$
1	$w = 7 \cdot 7^2 = 343 \equiv_{100} 43$
0	$w = 43^2 = 1849 \equiv_{100} 49$

Wartość liczby 7^{2022} modulo 100 to 49, więc przedostatnia cyfra liczby 7^{2022} to 4.

Przykład (drugi sposób)

Wyznaczyć przedostatnią cyfrę liczby 7^{2022}.
Zauważmy, że można uprościć obliczeniowo poprzednie rozwiązanie redukując wykładnik przy pomocy twierdzenia Eulera.

$$\varphi(100) = \varphi(2^2 \cdot 5^2) = 100 \cdot \frac{1}{2} \cdot \frac{4}{5} = 40 \quad \text{oraz} \quad 2022 = 40 \cdot 50 + 22.$$

Zatem

$$7^{2022} = 7^{40\cdot 50+22} = (7^{40})^{50} \cdot 7^{22} \equiv_{100} 1^{50} \cdot 7^{22} = 7^{22}.$$

Kontynuujemy zgodnie z algorytmem szybkiego potęgowania modularnego.
$22 = 10110_2$, więc rozpisujemy tabelę

1	$w = 7$
0	$w = 7^2 = 49$
1	$w = 7 \cdot 49^2 = 16807 \equiv_{100} 7$
1	$w = 7 \cdot 7^2 = 343 \equiv_{100} 43$
0	$w = 43^2 = 1849 \equiv_{100} 49$

Ponownie okazało się, że przedostatnią cyfrą liczby 7^{2022} jest cyfra 4.

Chińskie twierdzenie o resztach

Niech $m_1, m_2, \ldots, m_n \in \mathbb{N}/\{1\}$ będą parami względnie pierwsze oraz niech $r_1, r_2, \ldots, r_n \in \mathbb{Z}$. Wtedy układ równań

$$\begin{cases} x \equiv_{m_1} r_1 \\ x \equiv_{m_2} r_2 \\ \vdots \\ x \equiv_{m_n} r_n \end{cases}$$

ma dokładnie jedno rozwiązanie modulo $M = m_1 \cdot m_2 \cdot \ldots \cdot m_n$ postaci

$$x = N_1 M_1 + N_2 M_2 + \ldots + N_n M_n,$$

gdzie $M_i = \dfrac{M}{m_i}$ oraz N_i jest rozwiązaniem równania $M_i N_i \equiv_{m_i} r_i$ dla $i = 1, 2, \ldots, n$.

Oczywiście rozwiązania rozpatrywanego układu równań w zbiorze liczb całkowitych mają postać $x = N_1 M_1 + N_2 M_2 + \ldots + N_n M_n + Mt$, gdzie t jest dowolną liczbą całkowitą.

Przykład

Wyznaczyć najmniejszą liczbę naturalną spełniającą układ kongruencji
$\begin{cases} x \equiv_6 1 \\ x \equiv_{11} 6 \end{cases}.$
Zauważmy, że mamy $m_1 = 6$, $m_2 = 11$, $r_1 = 1$ i $r_2 = 6$.
Chińskie twierdzenie o resztach orzeka, że najmniejsze naturalne rozwiązanie układu jest liczbą mniejszą od 66.
$M_1 = 11$ i $M_2 = 6$. Otrzymujemy równania

$$11 \cdot N_1 \equiv_6 1 \ \text{ oraz } \ 6 \cdot N_2 \equiv_{11} 6.$$

Rozwiązaniami powyższych równań są $N_1 = 5$ oraz $N_2 = 1$. Zatem

$$x = 5 \cdot 11 + 1 \cdot 6 = 61.$$

Przykład

Wyznaczyć najmniejszą liczbę naturalną spełniającą układ kongruencji
$$\begin{cases} x \equiv_2 1 \\ x \equiv_3 1 \\ x \equiv_5 3 \end{cases}.$$
Z danych zadania otrzymujemy $m_1 = 2$, $m_2 = 3$, $m_3 = 5$, $r_1 = r_2 = 1$ oraz $r_3 = 3$.
Mamy $M_1 = 3 \cdot 5 = 15$, $M_2 = 2 \cdot 5 = 10$ oraz $M_3 = 2 \cdot 3 = 6$. Otrzymujemy równania
$$15 \cdot N_1 \equiv_2 1, \quad 10 \cdot N_2 \equiv_3 1, \quad 6 \cdot N_3 \equiv_5 3.$$
Rozwiązaniami powyższych równań są $N_1 = 1$, $N_2 = 1$ oraz $N_3 = 3$. Zatem
$$x = 1 \cdot 15 + 1 \cdot 10 + 3 \cdot 6 = 43 \equiv_{30} 13.$$
Ostatecznie najmniejszą liczbą naturalną spełniającą dany układ kongruencji jest 13.